underlying technology. Simultaneously the large ISPs are choosing to bypass the NAPs altogether and are instead engaging in "direct peering" at diverse locations. By leaving the NAPs to "the little guys," they are forcing the smaller ISPs to purchase transit via a third party to reach the larger ISPs, adding additional complexity and cost.

Pressure to Use to Private Peering Points: Better Problem Resolution

Networks that do not have direct peering relationships between each other either at a NAP or through direct peering, must rely on a third party to pass packets across most of the Internet. This inefficient architecture combined with the rapid growth of the Internet has created the following problems:

- "Trouble Ticket" reporting can involve at least three parties, instead of two, to manage a third party's problem. This creates a management bottleneck between ISPs. [7]
- A third party may not understand or be familiar with network issues of the two non-peering networks and may slow down the resolution of the network problem. This procedural bottleneck makes Internet network problems last longer.
- Packets may have to pass through the NAP two of more times. Once between non-peering ISPs and once to/from the third party. This greatly overloads the capacity of the NAP fabric and creates an unnecessary bottleneck. In addition, it increases the chances for packet loss at each NAP.

---

[6] http://www.fcc.gov/Bureaus/Common_Carrier/Comments/MFS WorldCom/Mar20/232136.wp (MCI Public Peering Policy). http://www.fcc.gov/Bureaus/Common_Carrier/Comments/MFS WorldCom/Mar20/233668.wp (UUNET's Northern American Peering Policy)

[7] A good example of this is the growing problem of unsolicited e-mail, commonly known as Span. Spammers know that they can hide behind layers of ISPs to send Spam to unsuspecting Internet customers. When the customers complain to the ISP, the response is that it was another provider who sent the Spam. That ISP will blame the next ISP along the tracer-route and so on to the originating ISP. By the time the situation is resolved by the ISP management, the Spammer may have very well moved on to a new obfuscated ISP.

An Attempt to Revitalize Some NAPs

At the same time that the 2nd and 3rd Tier providers are struggling for viability in this hostile market environment, several of the national backbone providers have proposed new private NAP facilities. In the May 1, 1998 edition of *Boardwatch*, a "brokered peering" proposal is set forth by several of the national backbone operators. They cite several reasons for launching better NAPs than are currently available. [8]

> "For all its improvement over public peering, the private peering system isn't perfect. One problem that hinders the transition from public to private peering is the cost of the additional local loops required to interconnect each network. For very large networks this cost is easily justified because the connections are filled with peering exchange data from their true peers. For smaller networks this cost becomes a barrier to entry to the privately peered network... Private peering has evolved as a rather exclusive club, generally available only between two NAPs that were clearly peers from the point of view of size and/or bandwidth exchanged. Smaller NAPs tended to get locked out of the private interconnection system because of the aforementioned lack of true peer definitions at the MAEs and NAPs. Over time, this exclusivity has created a two tiered system at the public MAEs and NAPs with the "good" bandwidth kept for true peers in private peering and the "not so good" bandwidth (due to its heavy congestion) left to the shared interconnect of the legacy MAE or NAP peers..."

The proposal goes on to suggest this devolution to "good" and "not so good" Internet bandwidth accelerated during the same period UUNET changed the peering landscape, with potentially disastrous results.

[8] www.boardwatch.com

"For many smaller NAPs the quantity and the quality of exchange bandwidth at the MAEs and NAPs decreased dramatically during 1997 compared to the overall growth in Internet bandwidth demand. This polarization of bandwidth quality impacts many users of the Internet, and threatens the diversity in the Internet that the multiplicity of service providers has created."

The four national backbone providers (Savvis, Electric Lightwave, Exodus, and Williams) making the brokered peering proposal document the failure of the current market to properly serve ISPs. They go on in their proposal to make recommendations that are helpful, but inadequate. They suggest Interconnection eXchanges (so called IXs) in cities that are already served by a NAP or interconnect exchanges. They establish a pecking order of at least three tiers (based on ISP size and facilities) at those interconnection points. The progress in removing barriers to high quality connections for all ISPs is small and there is no progress in serving cities not already served by a NAP or interconnection exchange. They also condone secret agreements -- a troublesome and far too widespread practice for agreements on interconnections.

Location of the NAPs and the Impact on Service

Many of the larger backbone providers have appeared unwilling to expand their backbone to regions beyond the large metropolitan areas. For example, today on the East Coast, many LATAs have no backbone to speak of. In these areas consumers face few alternatives. A few ISPs may lease expensive, usually under-sized, private trunks to a NAP, or their customers must dial long distance to reach the Internet, or dial an 800 number at higher ISP charges per minute.

or in the business case, pay increased costs for a private high-speed backbone connection. For customers in these areas, the Internet often appears to be slow to dial-up customers. It is often difficult to tell where the slowness comes from because it depends on the different levels of service along all the "hops" or linkages between the customer and the Internet site being contacted.

What would seem like the obvious answer to serving these outlying and undeserved areas is not so simple. Even though there is a great need for start-ups ISPs, there has been a steady elimination of incentives for entrance into the ISP business.

Serving Areas Distant From a Backbone or NAP

In the past, an ISP would interconnect with many ISPs primarily via MAE EAST or one of the other NAPS. Most ISPs were treated as equals in terms of how they were connected. There were many competitors to choose from with no one ISP dominating the landscape. In many situations there was an incentive to extend the Internet backbone into areas not well served by the larger ISPs. If, for example a small town in West Virginia was not being served by an existing ISP for either dial-up access or high-speed access, an entrepreneur might invest money and start up a local ISP. That ISP might purchase a high-speed backbone circuit to the closest NAP, and purchase transit to other ISPs at other NAPs. By doing so, the start-up ISP:

a. Created reliable affordable Internet access to customers in this small town.
b. Extended Internet access to a location that did not have access.

c. Permitted the flow of information within the local community.
d. Established local content creation via local web offerings.

Unfortunately, under today's partitioned quality regime on the Internet, there is no incentive for a start-up ISP to build a facility in West Virginia because of the costs associated with peering and the remoteness of nearby backbone connections. The economic viability of entering into non-Metropolitan areas with affordable, diversely routed, and high availability service is not sound. In essence, the barriers to entry have been raised too high. The prospect for a reasonable return on investment is slim considering the costs of doing business (pay for peering, long distance, high capacity data circuits) and the downward pressure on pricing to offer service at $20/month or less for unlimited access. Currently twenty-three LATAs in thirteen northeast/mid Atlantic states have no National Backbone point of presence, and only seven of those forty-one LATAs have a MAE or NAP or Interconnection exchange point.[9] (See diagram, page 30)

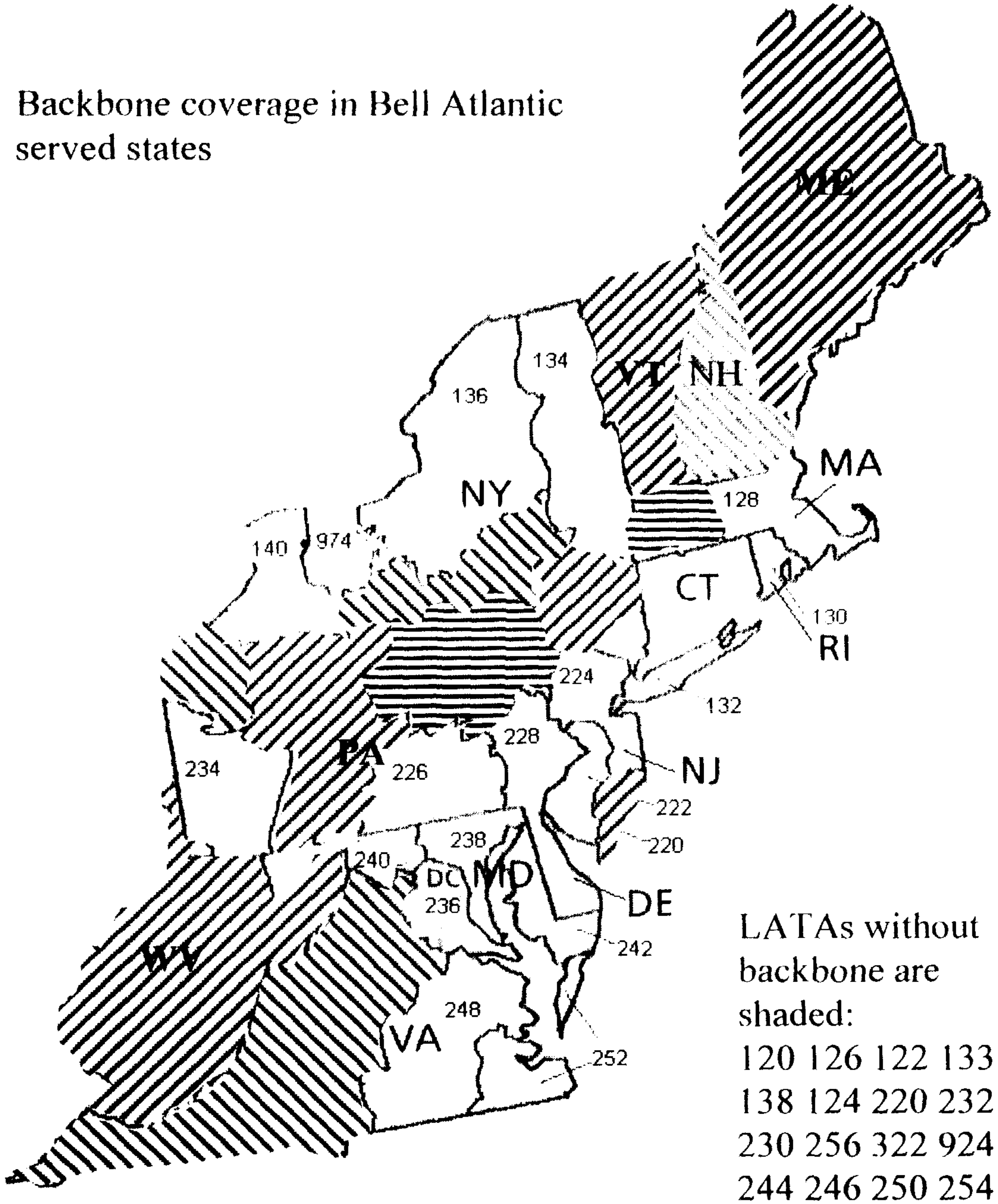
Even if you build it they may not come

There are a number of regionally based NAPs that have not become the core access points of the Internet for a variety of reasons. One of the primary reasons is that if major backbone providers are not exchanging packets at these locations, the utility of a NAP may be limited. The Routing Arbiter website tracks many small NAPs and interconnect exchanges that fall into this category.

---

[9] National backbone operators points of presence obtained from www.boardwatch.com. LATA maps were obtained from CCMI. The Routing Arbiter website, info.ra.net/div7/ra/, provided links to each of about 30 MAEs, NAPs, and IXs. Backbone POP cities and NAPs of all kinds were located on the LATA maps for ME, NH, VT, MA, RI, NY, NJ, PA, DE, MD, VA, DC, and WV

Backbone coverage in Bell Atlantic served states



LATAs without backbone are shaded:
120 126 122 133
138 124 220 232
230 256 322 924
244 246 250 254
927 928 929 932
951 956

Traffic volumes at many of these NAPs is very small, and the number of large ISPs who connect there is scant, if any.

The following is one survey of some of the non-MFS WorldCom owned NAPs across the US:

- The so-called "New York" NAP awarded by the NSF to Sprint, is actually located in Pennsauken, New Jersey a suburb of Philadelphia. To purchase a connection to Pennsauken requires at least one existing peering agreement at that NAP. MFS WorldCom has only a small presence (which has not been upgraded in a long time) and apparently peers with Sprint and ISPs based overseas. The growth and upgrade of the Pennsauken NAP has not kept up to the exponential growth of the Internet. However, it can be assumed that prices have not fallen.

- The Ameritech NAP located in Chicago has been slow to upgrade, limits access to competitive local carriers, and is located in a poor geographical place for Mid-US locations. However, the "Multiple Peering Level Agreement" started at this NAP was a good start, opening the way to establishing a more level playing ground for peering issues at this NAP.

- The NSF awarded the PAC-NAP to Pacific Bell, but because of too many changes of NAP managers (no one wanted the job), this NAP was late getting started and is now dwarfed by MFS WorldCom's competing MAE WEST.
- Another latecomer to the NAP business was the Palo Alto Internet Exchange (PAIX) administered by DEC. Being located at a legacy UUNET point-of-presence, it can hardly be called a "neutral" location.

The Price of Access

Prices for Internet services for consumers have come down, while barriers have increased for newer ISPs to participate fully at MAE EAST and MAE WEST. In order to peer at a NAP an ISP must purchase its local loop connection from WorldCom. These loops are typically $5000-$8000 per month. No price sheet exists, each price has to be quoted separately. WorldCom is firm on this. The loops must be purchased even if an ISP brings its connection to the room next door to the facility where WorldCom's connection is housed. Neither are LECs or CLECs exempt from Worldcom's mandatory purchase policy. In effect, MFS WorldCom has a near monopoly on providing 2nd Tier ISPs connectivity to the Internet.

The stated requirement to have multiple DS3s to at least 4 NAPs sets a price to "join the club," and generates marketing opportunity for large data circuit sales.[10] Even if the cost of peering was not there, each ISP must provision WorldCom circuitry into and out of the MAEs. This creates a unfair advantage to non-facilities based ISPs: they must purchase expensive, high speed circuits to these NAPs and pay significant revenue to WorldCom or other facility-based ISPs.

Secrecy as the Price of Peering

WorldCom, Sprint, and MCI are now charging for peering. Charging for peering creates a lower cost for WorldCom (et. al.) to connect to smaller ISPs and a corresponding increase in cost to the smaller ISP. WorldCom currently asks all peering ISPs to sign non-disclosure agreements (NDA). These NDAs effectively eliminate the ability to research what market prices are for peering with WorldCom. In addition, it allows WorldCom the ability to not charge some ISPs and to demand significant revenue from ISPs. While no hard evidence is currently available, it can be surmised that NASA and the Dept. of Energy are not charged for peering, but that other ISPs most likely are paying for the privilege of connecting to MFS WorldCom's (UUNET's) network.

[10] UUNET. "UUNET Details Peering Strategy: Changing Internet Economics Promote New Policy." Press Release. Online. Internet. 1 May. 1998.

With UUNET, ANS, CompuServe, MCI, and Gridnet all combining, it would seem that there would be very little peering except between small and overseas ISPs. Aside from the aggregation of once independent backbone operators now owned by MCI or MFS WorldCom, the following nine national backbone operators note that they too lease backbone facilities from MCI or MFS WorldCom: Concentric, GetNet, GlobalNet, Nap.NET, NetAccessUSA, Priori, Visinet, and Ziplink. [11]

[11] Boardwatch's database of National Backbone Operators. Through their lease agreements, MCI and WorldCom have an influence on pricing and transmission quality that is masked by the seemingly large diversity of names.

Conclusion

Current indicators are correct that the Internet is moving towards greater consolidation of ownership. This consolidation has resulted in a few large ISPs able to dictate the cost of doing business, the level of access and the quality of service for all of the other players or potential players. The geographic distribution of NAPs and backbone leaves many areas underserved – for both the ISPs and customers located there. At present there is no investor in Internet facilities significant enough to provide the price and geographic competition needed to restore a healthy marketplace for backbone capacity and NAPs.

By allowing large, willing investors such as the petitioning regional Bell companies into the backbone business, the FCC can help to break the stranglehold that the large ISPs have on network access. Authority to become regional providers of backbone service will benefit customers throughout their region with high-speed, high quality access to the Internet. The availability of massive amounts of regional backbone from these independent competitors to the 1st Tier ISPs will drive down the transit and peering prices faced by 2nd and 3rd Tier ISPs. The regional backbones will greatly improve the affordable, routing diversity options ISPs need to improve up-time and packet throughput. By approving this major improvement in the cost and availability of regional facilities, the FCC will do much to foster marketplace remedies that encourage more ISPs to enter the market and those already in it to improve the levels of service they offer customers. In order to correct the dangerous course that has been set for the Internet through the current trend towards consolidation, a course correction is needed. This course correction can best be achieved through the establishment of the following policies:

- Equal treatment of backbone providers.
- More NAPs with publicly available standards, low barriers to entry, and multiple different technical solutions.
- NAPs should be built where multiple carriers have significant facilities.
- NAPs should not be allowed to place restrictions on what carriers may provide service to the NAP.
- NAPs should be geographically dispersed, and located in reliable, safe, secure locations.
- The cost structure to provision a connection to the NAP should be as low as technically possible.
- NAPs should be located so that they are close to undersea cable landings.
- NAP ownership and administration should be completely removed from ISPs.
- NAPs should have incentives for growth and for meeting the needs of NAP customers and the Internet as a whole.
- Routing structures should be managed so that local packets are routed locally.
- Peering should be provided and encouraged for genuine educational and non-profit organizations if technically possible. Much of the Internet was developed with US taxpayer dollars as well as huge development funding from educational institutions.

Appendix of Terms[12]

Backbone: The principle high-speed circuits in which packets with ones network passes to reach customers and other networks.

IP: Abbreviation of Internet Protocol, pronounced as two separate letters. IP specifies the format of packets, also called datagrams, and the addressing scheme. Most networks combine IP with a higher-level protocol called Transport Control Protocol (TCP), which establishes a virtual connection between a destination and a source.

IP by itself is something like the postal system. It allows you to address a package and drop it in the system, but there's no direct link between you and the recipient. TCP/IP, on the other hand, establishes a connection between two hosts so that they can send messages back and forth for a period of time.

ISP: Short for Internet Service Provider, a company that provides access to the Internet, usually along with a variety of ancillary services.
In addition to serving individuals, ISPs also serve organizations of any size. ISPs themselves are connected to one another through Network Access Points (NAPs) and a variety of direct connections.

Internet: A global web connecting more than a million computers. Currently, the Internet has more than 50 million users worldwide, and that number is growing rapidly. More than 100 countries are linked into exchanges of data, news and opinions.

Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Its operators can choose which Internet services to provide to its local users and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well.

There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

MAE: **(Service Mark for MFS WorldCom)** originally stood for **Metropolitan Area Ethernet**, a Network Access Point (NAP) where Internet Service Providers (ISPs) can connect with each other. The original MAE was set up by a company called MFS and is based in Washington, D.C. Later, MFS built another one in Silicon Valley, dubbed MAE WEST. In

[12] http://www.pcwebopedia.com

addition to the MAEs from MFS, there are many other NAPs. Although MAE refers really only to the NAPs from MFS, the two terms are often used interchangeably.

NAP: Short for **Network Access Point**, a public networks exchange facility where Internet Service Providers (ISPs) can connect with one another in peering arrangements. The NAPs are a key component of the Internet backbone because the connections within them determine how packets are routed.

Packet: A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called *datagrams*.

Peering: A relationship between two or more ISPs in which the ISPs create a direct link between each other and agree to forward each other's packets directly. For example, suppose a client of ISP X wants to access a web site hosted by ISP Y. If X and Y have a peering relationship, the HTTP packets will travel directly between the two ISPs. In general, this results in faster access

Protocol: An agreed-upon format for transmitting data between two devices. The protocol determines the following: the type of error checking to be used

- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message

There are a variety of standard protocols from which programmers can choose. Each has particular advantages and disadvantages; for example, some are simpler than others are, some are more reliable, and some are faster.

Router: A device that connects two networks. Routers provide the ability to filter packets and forward them to different places based on various criteria. The Internet uses routers extensively to forward packets from one network to another.

Routing (how it works)
Routing is the process usually done with Routers that determine the path a packet takes to transverse the Internet.

Packet latency:
The time it takes (usually in milliseconds) for a particular packet to leave the source and arrive correctly at its destination. This is a complicated function of the speed-of-light, congestion on the backbone, and the distance the packet has to travel.

Peering session:

The logical router connection between two peers, usually at a NAP. The protocol "announces" to both parties, what networks they each want to accept packets for. The state-of-the-art protocol for this is BGP4.